541276

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
12. August 2004 (12.08.2004)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2004/068419 A1

(51) Internationale Patentklassifikation[7]: G07C 9/00, B60R 25/00

(21) Internationales Aktenzeichen: PCT/DE2003/003611

(22) Internationales Anmeldedatum:
30. Oktober 2003 (30.10.2003)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
103 01 146.3 14. Januar 2003 (14.01.2003) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **ROBERT BOSCH GMBH** [DE/DE]; Postfach 30 02 20, 70442 Stuttgart (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **PAVATICH, Frank** [AU/AU]; 2 Durban Court, Keilor Downs, Melbourne, VIC 3038 (AU). **ENGLEFIELD, Christopher, John, Chris** [AU/AU]; 45 Nicholson Street, Bentleigh, VIC 3204 (AU). **TSOLAKIS, Sophocles, Sam** [AU/AU]; 17 Gilles Street, Mitcham, VIC 3132 (AU).

(74) Gemeinsamer Vertreter: **ROBERT BOSCH GMBH**; Postfach 30 03 30, 70442 Stuttgart (DE).

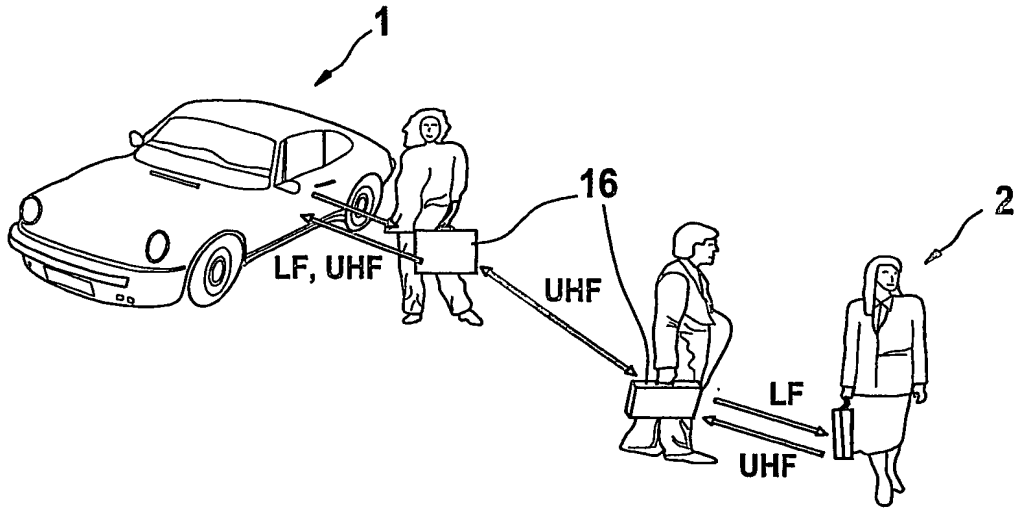
(81) Bestimmungsstaaten *(national)*: CN, KR, US.

(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

[Fortsetzung auf der nächsten Seite]

(54) Title: SECURITY SYSTEM

(54) Bezeichnung: EIN SICHERHEITSSYSTEM



(57) Abstract: The invention relates to a security system, including an electronic key (4) comprising a transmitter (6), and a secured object comprising a base station (8) with a receiver (10). The transmitter (6) and the receiver (10) are adapted to communicate for exchanging authentication data. The base station (8) regularly monitors the natural high-frequency (HF) signal level received by the receiver (10) and detects disturbances of the natural HF signal level, thereby enabling identification of a repeater (16).

(57) Zusammenfassung: Ein Sicherheitssystem, einschliesslich eines elektronischen Schlüssels (4), der einen Sender (6) aufweist, und eines gesicherten Objektes mit einer Basisstation (8), die einen Empfänger (10) aufweist. Der Sender (6) und der Empfänger (10) sind dazu ausgelegt zu kommunizieren, um Authentifizierungsdaten auszutauschen. Die Basisstation (8) überwacht regelmässig den seitens des Empfängers (10) empfangenen natürlichen Hochfrequenz (HF)-Signalpegel und erkennt Störungen des natürlichen HF Signalpegels, um eine Erkennung einer Relaisstelle (16) zu ermöglichen.

WO 2004/068419 A1

Veröffentlicht:
— *mit internationalem Recherchenbericht*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

EIN SICHERHEITSSYSTEM

Die vorliegende Erfindung bezieht sich auf ein Sicherheitsssystem, insbesondere ein passives Sicherheitssystem für Fahrzeuge.

Derzeit existierende passive Fahrzeug-Sicherheitssysteme für den Zugang oder die Inbetriebsetzung von Fahrzeugen verwenden fernbetätigte elektronische Schlüssel, die einen Sender einschließen, der Authentifizierungsdaten an einen in dem Fahrzeug befindlichen Empfänger übermittelt, wenn ein Transponder eines Schlüssels erregt wird, wenn sich der Schlüssel innerhalb eines vorbestimmten Bereichs des Empfängers befindet. Das zwischen dem Sender und dem Empfänger aktivierte Kommunikationsprotokoll benutzt eine Hochfrequenz-Schnittstelle zum Führen der übertragenen Daten sowie aller Daten, die von dem Fahrzeug an den Schlüssel gesandt werden. Die Hochfrequenz (HF)-Schnittstelle hat eine begrenzte Reichweite, um zu gewährleisten, dass die Kommunikationsverbindung unterbrochen wird, wenn sich eine im Besitz des Schlüssels befindliche Person aus der unmittelbaren Nähe des Fahrzeugs entfernt.

Passive Sicherheitssysteme sind leicht Angriffen unbefugter Personen ausgesetzt, die Abhör-Einrichtungen benutzen, welche in die Nähe des Fahrzeugs und des Schlüssels gebracht werden. Solche Einrichtungen werden dazu benutzt, den Schlüssel zu erregen, die von dem Schlüssel übermittelten Übertragungen zu empfangen und die Übertragungen an das Fahrzeug weiterzuübertragen. Die Abhör-Einrichtung, die vielfach eine oder mehrere Relaisstellen beinhaltet, umfaßt normalerweise einen Empfänger und einen Verstärker innerhalb des Bereichs des Schlüssels, um das abgefangene Signal an einen Empfänger und einen Verstärker in der Nähe des Fahrzeugs zu übertragen, um Zugang zu dem Fahrzeug zu erhalten.

Die Spezifikationen der australischen Patentanmeldungen 793933 und 42419/99 und 76313/01 beschreiben Sicherheitssysteme, welche eindeutige Zugriffsprotokolle für die Kommunikation zwischen dem Schlüssel und dem Fahrzeug verwenden, die zusätzlich zu der Übertragung der Authentifizierungsdaten verwendet werden können, um Angriffe seitens einer Relaisstelle zu erkennen oder zu verhindern. Das Zugriffsprotokoll ist das Kommunikationsprotokoll, welches ausgeführt wird, wenn der Schlüssel seitens des Fahrzeugs zur Kommunikation erregt oder getriggert wird. Das Zugriffsprotokoll

beinhaltet eine Anzahl von Prüfungen, die angewendet werden, um in der Erkennung der Relaisstelle behilflich zu sein, wie z.B. den in den Spezifikationen beschriebenen Zweitontest und den Übertragungssignalabweichungstest. Der Zweitontest insbesondere beruht auf Erkennung von Verzerrungsprodukten dritter Ordnung, die von der Relaisstelle erzeugt werden, und ist abhängig von der Linearität der in der Relaisstelle verwendeten Verstärker und Mischer. Da mittlerweile jedoch hoch lineare Verstärker und Mischer zur Verfügung stehen, ist es schwierig, von der Relaisstelle erzeugte Verzerrungsprodukte dritter Ordnung zu erkennen. Es ist daher wünschenswert, eine andere Technik vorzustellen, die einen Relaisstellenangriff erkennt oder bei der Erkennung eines solchen behilflich ist.

Die vorliegende Erfindung stellt ein Sicherheitssystem vor, einschließlich eines elektronischen Schlüssels, der einen Sender aufweist, und eines gesicherten Objektes mit einer Basisstation, die einen Empfänger aufweist, wobei der Sender und der Empfänger so ausgelegt sind, dass sie miteinander kommunizieren, um Authentifizierungsdaten auszutauschen, dadurch gekennzeichnet, dass

die Basisstation regelmässig den seitens des Empfängers empfangenen natürlichen Hochfrequenz (HF)-Signalpegel überwacht; und

dass die Basisstation Störungen des natürlichen HF-Signalpegels erkennt, um eine Erkennung einer Relaisstelle zu ermöglichen.

Die vorliegende Erfindung stellt auch eine von einem Sicherheitssystem durchgeführte Kommunikationsmethode vor, einschließlich eines elektronischen Schlüssels, der einen Sender aufweist, und eines gesicherten Objektes mit einer Basisstation, die einen Empfänger aufweist, wobei die Methode die Übertragung von Authentifizierungsdaten von dem Sender an den Empfänger einschließt, dadurch gekennzeichnet, dass die Basisstation:

den seitens des Empfängers empfangenen natürlichen Hochfrequenz (HF)-Signalpegel überwacht; und

Störungen des natürlichen HF Signalpegels erkennt, um eine Erkennung einer Relaisstelle zu ermöglichen.

Eine bevorzugte Realisierung der vorliegenden Erfindung ist nur beispielsweise nachfolgend mit Bezug auf die beiliegenden Zeichnungen beschrieben:

Figur 1 ist eine schematische Darstellung eines Relaisstellenangriffs;
Figur 2 ist eine schematische Darstellung einer bevorzugten Ausführung eines Sicherheitssystems, und einer Relaisstelle;
Figur 3 ist ein Blockdiagramm des Sicherheitssystems;
Figur 4 ist ein Flussdiagramm eines Kontrollprozesses einer Basisstation des Sicherheitssystems.

Ein gesichertes Objekt, wie z.B. ein Fahrzeug 1 wie in Figur 1 gezeigt, ist mit einem passiven Sicherheitssystem ausgerüstet, welches einem berechtigten Benutzer 2, der einen Schlüssel 4 bei sich trägt, Zugriff und Benutzung des Fahrzeugs 1 genehmigt, wenn der Schlüssel 4 sich in einem vorherbestimmten Bereich des Fahrzeugs 1 befindet. Ein Relaisstellenangriff kann unternommen werden, um ohne die Genehmigung des berechtigten Benutzers Zugang zu dem Fahrzeug zu erlangen, und zwar unter Verwendung von Abhör-Einrichtungen, welche eine oder mehrere Relaisstellen 16 umfassen. Der Benutzer 2 des Fahrzeugs 1 kann im Besitz des Schlüssels sein, und eine erste Relaisstelle 16 kann dazu benutzt werden, den Schlüssel zu erregen und eine Übertragung seitens des Schlüssels gemäss dem Zugriffsprotokoll aufzurufen. Die Signale des Schlüssels werden an eine weitere Relaisstelle 16 weiterübertragen, die von einem Angreifer in der Nähe des Fahrzeugs bereitgehalten wird. Die zweite Relaisstelle 16 überträgt wiederum die Signale weiter an das Fahrzeug 1. Dadurch wird eine Kommunikationsverbindung zwischen dem Schlüssel und dem Fahrzeug 1 hergestellt, obwohl sich der Besitzer nicht in dem vorherbestimmten Bereich des Fahrzeugs befindet, was normalerweise erforderlich ist, um das Zugriffsprotokoll aufzurufen.

Das passive Sicherheitssystem, wie in den Figuren 2 und 3 gezeigt, umfaßt einen elektronischen Schlüssel 4 mit einem Sender 6 und einer Sendeantenne 7, einer Basisstation 8 mit einem Empfänger 10 und Empfangsantenne 12. Die Basisstation 8 ist in einem gesicherten Objekt untergebracht, wie z.B. dem Fahrzeug 1, und kontrolliert den Zugang zu dem gesicherten Ort und/oder zum Starten des Fahrzeugs. Wenn der Schlüssel 4 innerhalb eines bestimmten Bereichs an die Antenne 12 des Empfängers 10 herangeführt wird, erregt der Empfänger 10 den Transponder des Schlüssels 4 oder wird getriggert, diesen zu erregen, und veranlaßt dadurch den Sender 6, die Übermittlung an den Empfänger 10 zu beginnen. Die Daten werden unter Verwendung von HF-Signalen übermittelt, welche eine Kommunikationsverbindung zwischen dem Schlüssel 4 und der

Basisstation 8 herstellen. Die zwischen dem Schlüssel 4 und der Basisstation 8 übermittelten Daten werden durch ein Kommunikationszugriffsprotokoll bestimmt, welches der Schlüssel 4 und die Basisstation 8 befolgen, und welches die Übermittlung von Authentifizierungsdaten von dem Schlüssel 4 an den Empfänger 10 beinhaltet. Ein Zugang zu dem gesicherten Bereich und/oder zum Starten des Fahrzeugs wird von der Basisstation 8 nur dann zugelassen, wenn die übermittelten Authentifizierungsdaten mit den von der Basisstation 8 gespeicherten Authentifizierungsdaten übereinstimmen.

Der Schlüssel 4 und die Basisstation 8 umfassen eine Reihe von Sicherheitsmerkmalen, wie z.B. diejenigen, die in den Zugriffsprotokoll-Spezifikationen beschrieben sind. Die Bauteile des Schlüssels 4 und der Basisstation 8 sind dieselben wie in den Zugriffsprotokoll-Spezifikationen beschrieben, mit der Ausnahme, dass ein Mikrocontroller 40 der Basisstation 8 so ausgelegt ist, dass ein Kontrollprozess wie untenstehend mit Bezug auf Figur 4 beschrieben, ausgeführt wird. Dies kann erzielt werden durch Einstellen der Steuer-Software des Mikrocontrollers 40 und/oder Einbau eines anwendungsspezifischen integrierten Schaltkreises (ASIC) als Teil des Mikrocontrollers 40, um zumindest einen Teil des Kontrollprozesses durchzuführen.

Der Schlüssel 4 schließt einen Mikrocontroller 35 ein, der die Steuer-Software zur Steuerung der Schlüsselkomponenten als Teil des Kommunikationsprotokolls umfaßt. Der Mikrocontroller 35 steuert den Sender 6, welcher einen ersten Oszillator 30 zur Erzeugung eines ersten Grundtons 60 und einen zweiten Oszillator 32 zur Erzeugung eines zweiten Grundtons 62 einschließt. Die erzeugten Frequenzsignale werden von einem Kombinator (Antennenweiche) oder Summierverstärker 34 für die Übertragung durch die UHF-Sendeantenne 7 kombiniert. Der Mikrocontroller 35 ist auch zur Steuerung der Oszillatoren 30 und 32 angeschlossen, so dass er einen Frequenzversatz oder eine Frequenzabweichung, gestützt auf die zu übertragenden Daten, bewirken kann. Der Mikrocontroller 35 ist auch geeignet, Steuerdaten von der Basisstation 8 über einen Niederfrequenz-Empfänger 9 und eine Antenne 31 zu empfangen. Der Schlüssel 4 schließt eine Transponderschaltungsanordnung 9 ein, um den Schlüssel 4 zu erregen oder zu triggern, wenn er sich innerhalb eines vorbestimmten Bereichs der Basisstation 8 befindet. Innerhalb dieses Bereichs kann ein Erregungssignal seitens des Fahrzeugs erzeugt werden, wenn ein bestimmtes Ereignis eintritt, wie z.B. das Anheben des Türgriffes oder ähnliches.

Sobald der Schlüssel 4 erregt oder aktiviert ist, wird das Kommunikationsprotokoll 4 für die Zugriffsberechtigung des Fahrzeugs in Gang gesetzt.

Die Basisstation 8 umfasst einen Mikrocontroller 40, der Steuer-Software aufweist und welcher den Betrieb der Komponenten der Basisstation 8 steuert. Diese Teile umfassen einen UHF-Empfänger 36, der mit der Empfangsantenne 12 verbunden ist, um eine Ausgabe der für den Mikrocontroller 40 empfangenen Daten bereitzustellen. Ein Analog/Digital-Umsetzer 38 wird verwendet, um die analogen Ausgangssignale des Empfängers 36 in eine digitale Form für den Mikrocontroller 40 umzusetzen. Diese Signale schließen eine RSSI (Eingangssignalstärkenanzeiger)- Ausgabe ein, welche spektrale Signaturdaten für den Mikrocontroller 40 bereitstellt. Zwischenfrequenzsignale, die von dem Empfänger 36 erzeugt werden, werden an ein Filter 43 weitergeleitet und dann an den Empfänger 36 zurückgeleitet, um die in den Signalen enthaltenen Daten herauszufiltern. Die Filter 43 sind geschaltete ("switched") Zwischenfrequenzfilter mit Bandbreiten, die von dem Mikrocontroller 40 in Übereinstimmung mit dem Zugriffsprotokoll eingestellt werden. Die Basisstation 8 hat auch einen Niederfrequenzsender 37 und eine Antenne 39 zur Übertragung von Daten von dem Mikrocontroller 40 an den Schlüssel 4. Der Niederfrequenzsender 37, die Antennen 39 und 31 und der Niederfrequenz-Empfänger 9 sind so ausgelegt, dass eine Niederfrequenz-Kommunikationsverbindung nur dann hergestellt wird, wenn der Schlüssel 4 und die Basisstation 8 gemeinsam innerhalb des gesicherten Bereichs untergebracht sind, z.B. innerhalb des Fahrzeugs. Dazu kann die Sendeantenne 39 zum Beispiel in Form einer Spule ausgebildet sein, die in einem Zündsystem untergebracht ist, so dass eine Verbindung nur dann mit der Antenne 31 hergestellt wird, wenn der Schlüssel 4 in den Zündschalter des Zündsystems eingeführt wird. Die Niederfrequenzkanal-Verbindung wird benutzt, um Synchronisationskontrolldaten von der Basisstation an den Schlüssel 4 zu senden, damit diese verwendet werden können, wenn der Schlüssel 4 das nächste Mal erregt wird. Die Synchronisationskontrolldaten werden dazu benutzt, die Zeiten für die verschiedenen Teile oder Komponenten der in dem Zugriffsberechtigungsprotokoll übersandten Nachrichten einzustellen.

Das Zugriffsprotokoll bedient sich einer Reihe von Techniken, um einen Relaisstellenangriff, inbesondere die Störung seitens einer eventuell vorhandenen Relaisstelle 16 zu erkennen. Diese Techniken umfassen einen Zweitontest, der auf dem

Pegel der Intermodulationsverzerrungsprodukte dritter Ordnung, die von der Basisstation 10 empfangen werden und mit der Übertragung der Grundtöne der Oszillatoren 30 und 32 verbunden sind, basiert. Diese Techniken beinhalten auch Zeitabläufe, Leistung und Frequenzabweichungen, die in der Übertragung der Authentifizierungsdaten verwendet werden und Bestandteil des Kommunikationszugriffsprotokolls darstellen. Eine Reihe von Prüfungen werden von dem Mikrocontroller 40 basierend auf den als Teil des Zugriffsprotokolls empfangenen Daten durchgeführt. Ist eine Bedingung der Prüfung erfüllt, so wird ein Sicherheitsmerker für den betreffenden Test im Mikrocontroller 40 gesetzt. Der Status der im Mikrocontroller vorhandenen Merker dient der Feststellung, ob eine Relaisstelle 16 vorhanden ist und insbesondere ob Zugang zu dem Fahrzeug gewährt werden soll. Zur Unterstützung dieser Techniken führt die Basisstation 8 einen weiteren kontinuierlichen Test durch, der nachstehend als "Rauschtest" bezeichnet wird.

Der Rauschtest stützt sich auf die Erkennung von Störungen oder abrupten Änderungen im Ausmaß des Hochfrequenzrauschens im natürlichen Umfeld der Basisstation 8 des Fahrzeugs 1. Alle Relaisstellen 16, die eine Hochfrequenzverstärkung benutzen, ungeachtet der Linearität ihrer Verstärker, werden nicht nur die Signale verstärken, die im Zugriffsprotokoll von Interesse sind, sondern auch jegliches HF-Rauschen innerhalb des Durchlassbandes der Relaisstelle 16. Der Umfang der Verstärkung ist abhängig von dem gesamten Verstärkungsgrad der durch eine Relaisstelle hergestellten Verbindung, und je höher der Verstärkungsgrad der Verbindung, desto höher die Wahrscheinlichkeit einer Erkennung.

Um die Erkennungstechniken des Zugriffsprotokolls voll auszunutzen, weist das Durchlassband der Basisstation 8 eine genügende Bandbreite auf, so dass es in eine Anzahl von Kanälen unterteilt werden kann. Die Mindestdurchlassbandbreite einer jeden Relaisstelle 16 wird normalerweise größer als die der Basisstation 8 oder dieser gleich sein. Wenn eine Relaisstelle 16 aktiviert wird, wird das Ausmaß des Rauschens im Durchlassband der Relaisstelle erhöht. Dies kann dadurch erkannt werden, dass die Basisstation 8 jegliche Änderung des DC Rauschpegels im gesamten Durchlassband überwacht.

Die Basisstation 8 ist in der Lage, den Rauschtest anhand des in Figur 4 gezeigten Kontrollprozesses durchzuführen. Der Prozess beginnt bei Schritt 41, wenn die

Basisstation 8 erkannt hat, dass der Motor des Fahrzeugs abgestellt worden ist und der Benutzer das Fahrzeug auf reguläre Weise verlassen hat, und zwar durch Verriegeln des Fahrzeugs oder dadurch, dass der Schlüssel aus der Nähe des Fahrzeugs entfernt worden ist. Bei Schritt 41 löscht der Mikrocontroller 40 alle seine Sicherheitsmerker für die Relaissstellenangriffserkennung und bei Schritt 42 wird ein Zeitgeber T auf 0 gestellt. Der Zeitgeber T mißt die verstrichene Zeit kontinuierlich in Sekunden. Bei Schritt 44 entnimmt der Mikrocontroller Stichproben der RSSI (Eingangssignalstärkenanzeiger)-Ausgabe des UHF Empfängers 36 (über den A/D-Umsetzer 38) um Datenstichproben über sein gesamtes Durchlassband für die empfangenen Signale an einer Anzahl von Frequenzkanälen zu erhalten.

Falls zum Beispiel das Durchlassband der Basisstation 8 bei 1,6 MHz liegt und die RSSI-Ausgabe in der Lage ist, dieses Band in 100 kHz Kanäle zu unterteilen, dann können 16 Datenstichproben über das gesamte Durchlassband für die entsprechenden Kanäle erhalten werden. Bei Schritt 44 sammelt der Mikrocontroller 40 eine Anzahl von Datenstichproben x[n], z.B. 20, für jeden Frequenzkanal und diese werden bei Schritt 45 zur Erfassung eines Mittelwertes $\bar{x}[n]$ verwendet. Der Mittelwert $\bar{x}[n]$ wird als ein Frequenz-Binwert für jeden Kanal in einem entsprechenden Zwischenspeicher des Mikrocontrollers 40 gespeichert. Die Zwischenspeicher sind auf eine Größe eingestellt, die es ermöglicht, eine ausgewählte Aufzeichnung von Mittelwerten aufrechtzuerhalten.

Der Rauschtest wird bei Schritt 46 durchgeführt. Der Rauschtest kann sehr einfach sein und darin bestehen, dass festgestellt wird, ob eine ausgewählte Anzahl der Frequenzbins einen Binwert haben, der über einem vorherbestimmten Schwellenwert liegt. Falls zum Beispiel die gegenwärtigen Daten $\bar{x}[n]$ für 13 der 16 Bins über einem vorherbestimmten Schwellenwert liegt, dann kann der Rauschtest als seine Bedingungen erfüllt zu haben betrachtet werden. Alternativ können die Rauschtestbedingungen auch als erfüllt betrachtet werden, falls eine Anzahl vergangener $\bar{x}[n]$ Stichproben den Schwellenwert überschritten haben. Vorzugsweise wird der Rauschtest nur als zufriedenstellend betrachtet, falls eine Anzahl der Kanäle die Schwelle überschreiten und eine Anzahl weitere für jene Kanäle gesammelte Stichproben bestätigen, dass der Schwellenwert tatsächlich überschritten worden ist. Die zusätzlichen Stichproben werden gemacht, um die Wahrscheinlichkeit falscher Erkennung zu vermindern. Es wird angenommen, dass ein legitimer Störender,

der sich nicht einer Relaisstelle bedient, nicht ein ganzes Durchlassband für eine Relaisstelle belegen würde, und daher nur einen oder zwei der Frequenzkanäle stören würde.

Der Pegel des Schwellenwertes ist dynamisch. Er wird festgestellt durch Stichproben des HF-Umfeldes sofort nachdem der Motor abgeschaltet worden ist und das Fahrzeug auf reguläre Art und Weise verlassen worden ist, gemäss Schritt 41. Wenn der Schwellenwert auf der Basis dieser HF-Umfeld-Stichprobe eingestellt worden ist, werden gemäß Schritt 41 alle Frequenzbins neu eingestellt.

Eine weitere alternative Methode zur Durchführung des Rauschtests beruht auf dem Prinzip, dass das HF-Rauschen als weißes Rauschen betrachtet wird und deshalb gemäß einer Gaußschen Wahrscheinlichkeitsdichtefunktion (PDF) verteilt ist. Um Störungen zu erkennen, die eine Steigerung im mittleren weißen Rauschpegel (oder DC Pegel) betrifft, führt der Mikrocontroller 40 eine Wahrscheinlichkeitsdichtefunktion aus, wobei A die Steigerung im DC Pegel des weißen Gaußschen Rauschens ist. Diese Wahrscheinlichkeitsdichtefunktion p stellt (gestützt auf die Stichprobendaten) die Wahrscheinlichkeit fest, dass ein bestimmter Signalpegel A erreicht worden ist. Diese von dem Mikrocontroller 40 ausgeführte Wahrscheinlichkeitsdichtefunktion lautet:

$$p(x;A)=\frac{1}{\sqrt{(2\pi\sigma^2)^N}}\exp\left[-\frac{1}{2\sigma^2}\sum_{n=0}^{N-1}(x[n]-A)^2\right]$$

Dabei ist:

"n" = die Stichprobe, der die Daten entnommen werden,

"N" = die Anzahl der Stichproben, die für einen Frequenzkanal entnommen worden sind,

"x" = die Stichprobendaten,

"σ^2" = die Varianz von x,

"A" = der Signalpegel des weißen Gaußschen Rauschens.

Der Mikrocontroller 40 kann die Wahrscheinlichkeitsdichtefunktion (PDF) durchführen, so dass nach A oder nach der Wahrscheinlichkeit p aufgelöst wird. Wenn der Mikrocontroller die Wahrscheinlichkeit p auf einen festen Wert einstellt, dann wird ein Wert von A für diese Wahrscheinlichkeit unter Verwendung der Wahrscheinlichkeitsdichtefunktion (PDF) festgelegt. Die Wahrscheinlichkeit kann hoch

genug eingestellt werden, um falsche Erkennung zu minimieren. Zum Beispiel weist ein p von 0,9 darauf hin, dass mit hoher Wahrscheinlichkeit der Pegel A erreicht worden ist, wohingegen ein p von 0,5 eine weitaus geringere Sicherheit bedeutet. Der von der Wahrscheinlichkeitsdichtefunktion (PDF) erhaltene Wert A wird als dynamischer Schwellenwert gegenüber einem Messwert für A, der direkt von den Stichprobendaten erhalten wird, eingesetzt. Der Messwert für A kann ein Durchschnitt über alle Stichproben in den Frequenzbins oder ein Durchschnitt über einige Frequenzbins sein. Wenn der Messwert für A den von der Wahrscheinlichkeitsdichtefunktion (PDF) festgelegten Schwellenwert für A überschreitet, dann werden die Rauschtestbedingungen als erfüllt betrachtet. Alternativ können die Stichprobendaten verwendet werden, um einen Wert für A zu erhalten, und dann können die Stichprobendaten und der Wert für A in der Wahrscheinlichkeitsdichtefunktion (PDF) verwendet werden, die von dem Mikrocontroller 40 ausgeführt wird, um Messwerte für p bei verschiedenen Zeitabständen zu erzeugen. Für jeden Messwert von p, der von dem Mikrocontroller 40 bei Schritt 46 festgestellt wird, wird dieser dann mit einem festgelegten Schwellenwert für p, zum Beispiel 0,7, verglichen; und falls der Messwert für p den Schwellenwert überschreitet, werden die Rauschtestbedingungen als erfüllt angesehen.

Die Wahrscheinlichkeitsdichtefunktion (PDF) hat den Vorteil, dass sie jegliche Spitzen, die durch Zufallsereignisse eingeführt werden, herausfiltert, ist aber andererseits für den Mikrocontroller 40 rechnerisch aufwendig. Die Wahrscheinlichkeitsdichtefunktion (PDF) kann auch als eine weitere Überprüfung eingesetzt werden, sobald der anfängliche Stichprobenschwellentest positiv war und anzeigt, dass eine Relaisstelle 16 vorhanden ist.

Bei Schritt 48 wird festgestellt, ob die Rauschtestbedingungen erfüllt worden sind. Falls dies der Fall ist, wird der Sicherheitsmerker für das Rauschen bei Schritt 50 gesetzt. Die Schritte 42 bis 48 sollten alle innerhalb von Millisekunden durchgeführt werden. Im Schritt 52 wird festgestellt, ob T eine Abtastzeit von y Sekunden, z.B. 10 Sekunden, erreicht hat. Falls nicht, durchläuft der Kontrollprozess eine Schleife, wobei er kontinuierlich ein Triggersignal sucht, um die Kommunikation mit dem Schlüssel 4, bei Schritt 54, einzuleiten. Das Triggersignal kann ein Einleitungssignal sein, welches durch Anheben eines der Türgriffe oder Aktivierung eines Türgriffaktuators verursacht wird, oder ein Signal, welches generiert wird, wenn die Zündung zum Starten des Motors aktiviert wird.

Falls kein Triggersignal empfangen wird, versucht der Kontrollprozess durch Prüfen des Wertes von T bei Schritt 52 festzustellen, ob y Sekunden vergangen sind. Falls ein Triggersignal empfangen wird, führt der Mikrocontroller 40 bei Schritt 56 seinen Teil des Zugriffsprotokolls aus.

Falls der Zeitgeber T in Schritt 52 y Sekunden erreicht hat wird eine kontinuierliche Schleife erregt und die Schritte 40 bis 48 durchgeführt, so dass ein weiterer Satz von Binwerten für die Zwischenspeicher des Controllers 40 zur Verfügung steht. Demgemäß führt die Basisstation 8 alle y Sekunden Stichproben der Rauschpegel über das Durchlassband durch.

Wenn das Zugriffsprotokoll durchgeführt wird (Schritt 56) besteht ein Teil des Protokolls letztendlich darin zu bestimmen, ob Zugriff auf das Fahrzeug 1 oder Benutzung desselben gewährt oder genehmigt werden soll. Als Teil dieser Bestimmung werden die Sicherheitsmerker überprüft, und der Status der Rauschmerker dient der Ermittlung, ob eine Relaisstelle 16 vorhanden ist und in einem Relaisstellenangriff benutzt wird. Der Zugriff kann versagt werden, falls der Rauschmerker gesetzt ist oder falls einer oder mehrere der Sicherheitsmerker gesetzt sind. Zugriff wird eventuell zum Beispiel nur dann versagt, falls drei der Merker gesetzt sind.

Der von der Basisstation durchgeführte Rauschtest bietet bedeutende Vorteile dadurch, dass er dynamisch selbstanpassend an das HF-Umfeld in der Nähe der Empfangsantenne 12 des Fahrzeugs erfolgt. Die Ermittlungstechnik ist tolerant in Bezug auf Störungen, die nicht von einer Relaisstelle herrühren. Auch können die festgehaltenen Frequenzbinwerte dazu verwendet werden, einen bevorzugten Kanal für die Datenkommunikation mit dem Schlüssel 4 festzulegen.

Dem Fachkundigen werden hierzu eine Vielzahl von Abwandlungen gegenwärtig werden, ohne dass der Umfang der vorliegenden Erfindung, wie sie hiermit unter Bezug auf die beiliegenden Zeichnungen beschrieben wurde, überschritten wird.

PATENTANSPRÜCHE:

1. Ein Sicherheitssystem, einschließlich eines elektronischen Schlüssels (4), der einen Sender (6) aufweist, und eines gesicherten Objektes mit einer Basisstation (8), die einen Empfänger (10) aufweist, wobei der Sender (6) und der Empfänger (10) so ausgelegt sind, dass sie miteinander kommunizieren, um Authentifizierungsdaten auszutauschen, dadurch gekennzeichnet, dass

   die Basisstation (8) regelmässig den seitens des Empfängers (10) empfangenen natürlichen Hochfrequenz (HF)-Signalpegel überwacht; und

   dass die Basisstation (8) Störungen des natürlichen HF-Signalpegels erkennt, um eine Erkennung einer Relaisstelle (16) zu ermöglichen.

2. Ein Sicherheitssystem nach Anspruch 1, in welchem die Basisstation (8) Stichproben des über eine Mehrzahl von Frequenzkanälen des Empfängers (10) empfangenen HF-Signalpegels generiert.

3. Ein Sicherheitssystem nach Anspruch 2, in welchem die Basisstation (8) einen auf den Stichproben basierenden Rauschtest durchführt, um die Störung zu erkennen.

4. Ein Sicherheitssystem nach Anspruch 3, in welchem die Rauschtestbedingungen als erfüllt gelten, wenn eine Anzahl der Stichproben einen vorherbestimmten Schwellenwert überschreiten.

5. Ein Sicherheitssystem nach Anspruch 3, in welchem der Rauschtest basierend auf einer von den Stichproben hergeleiteten Gaußschen Wahrscheinlichkeitsdichtefunktion bestimmt wird.

6. Ein Sicherheitssystem nach Anspruch 1, in welchem die Basisstation (8) über eine Zeitdauer eine Anzahl der Stichproben für jeden der Frequenzkanäle festhält, um den natürlichen HF-Signalpegel darzustellen.

7. Ein Sicherheitssystem nach Anspruch 1, in welchem die Basisstation (8) und der Schlüssel (4) ein Zugriffsprotokoll zur Übertragung der Authentifizierungsdaten

ausführt und das Zugriffsprotokoll die Bestimmung einschließt, ob Zugriff und/oder Benutzung des gesicherten Objekts basierend auf dem Rauschtest gewährt werden soll.

8. Ein Sicherheitssystem nach einem beliebigen der vorhergehenden Ansprüche, in welchem das gesicherte Objekt ein Fahrzeug (1) ist.

9. Eine von einem Sicherheitssystem durchgeführte Kommunikationsmethode, einschließlich eines elektronischen Schlüssels (4), der einen Sender (6) aufweist, und eines gesicherten Objektes mit einer Basisstation (8), die einen Empfänger (10) aufweist, wobei die Methode die Übertragung von Authentifizierungsdaten von dem Sender (6) an den Empfänger (10) einschließt, dadurch gekennzeichnet, dass die Basisstation (8):

den seitens des Empfängers (10) empfangenen natürlichen Hochfrequenz (HF)-Signalpegel überwacht; und

Störungen des natürlichen HF Signalpegels erkennt, um eine Erkennung einer Relaisstelle (16) zu ermöglichen.

Fig. 1

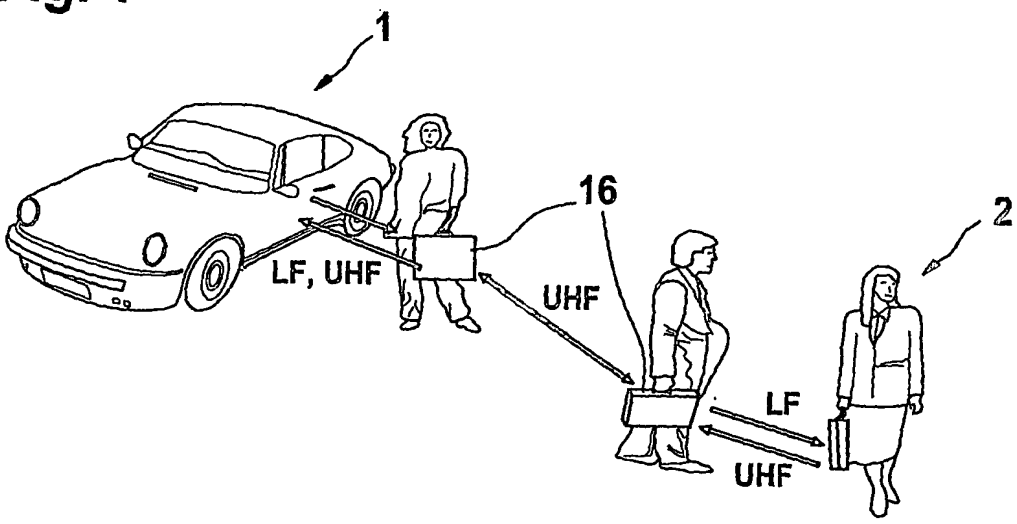


Fig. 2

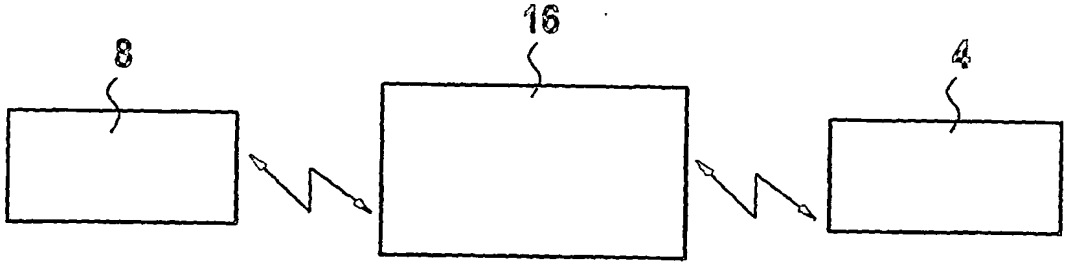


Fig. 3

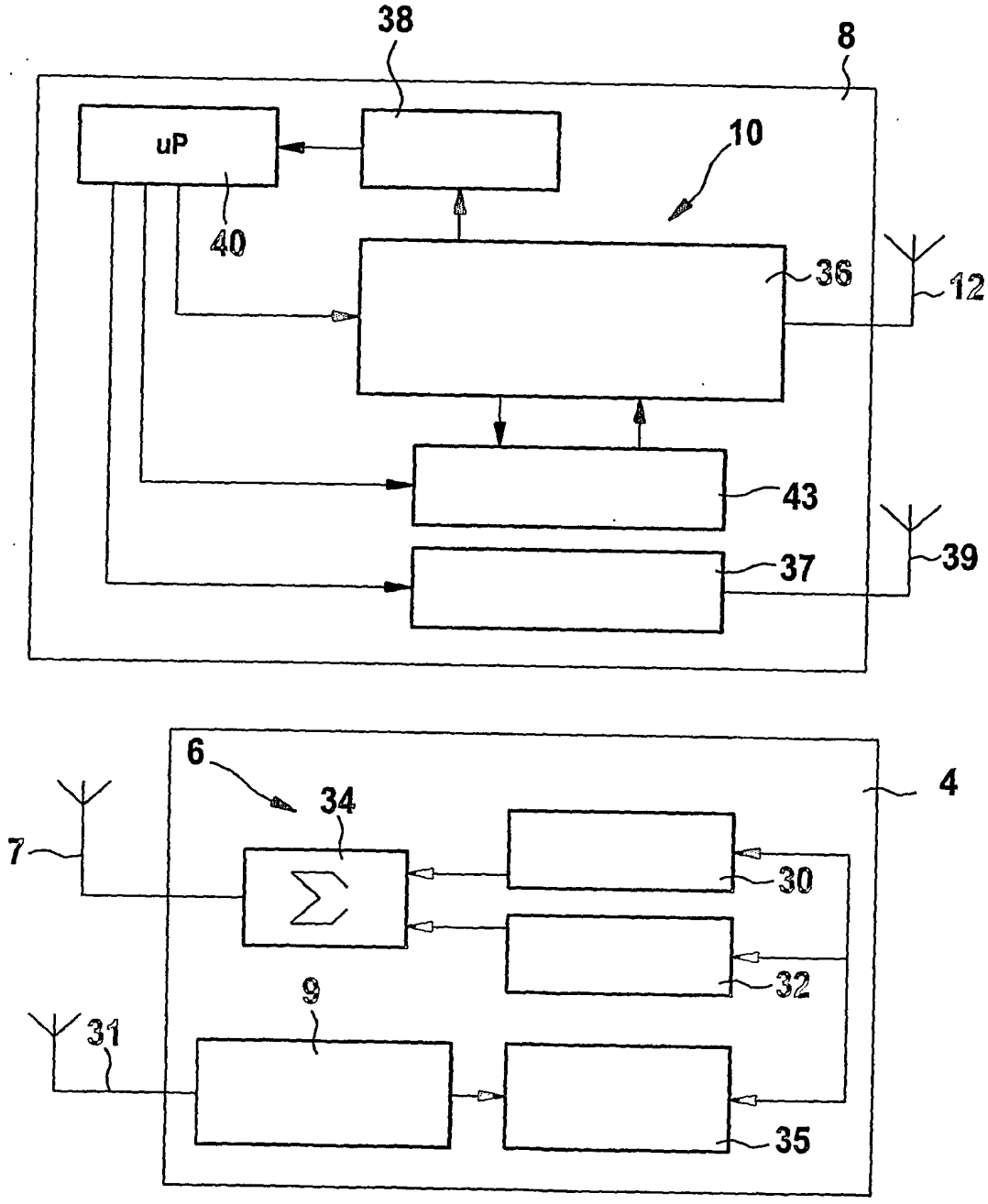
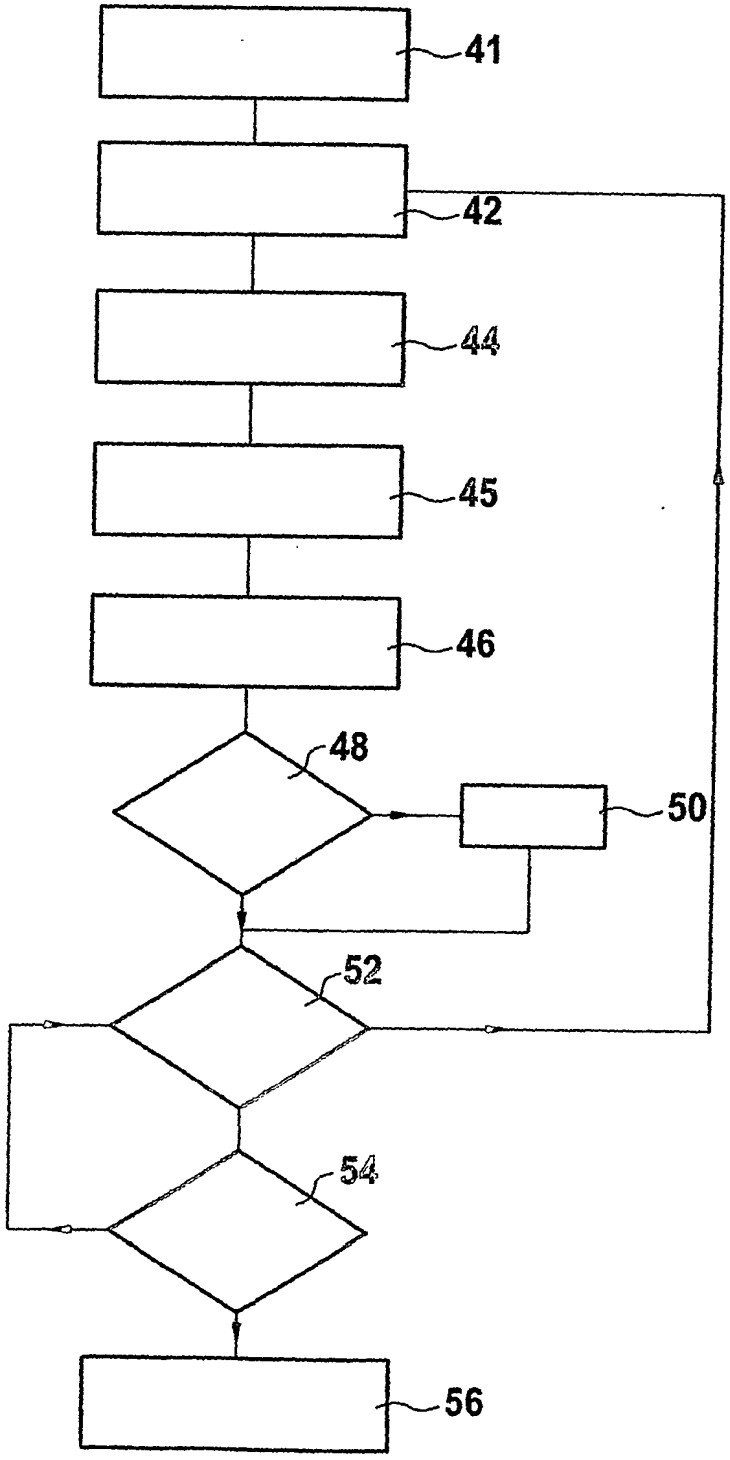


Fig. 4



INTERNATIONAL SEARCH REPORT

International Application No
PCT/DE 03/03611

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07C9/00 B60R25/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07C B60R

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 02/17238 A (CROWHURST PETER ; PAVATICH FRANK (AU); BOSCH GMBH ROBERT (DE)) 28 February 2002 (2002-02-28) cited in the application the whole document	1-9
A	WO 00/05696 A (PAVATICH GIANFRANCO ; CROWHURST PETER (AU); BOSCH GMBH ROBERT (DE)) 3 February 2000 (2000-02-03) the whole document	1-9
A	WO 02/49888 A (GREENWOOD JEREMY JOHN ; LAND ROVER (GB); HI KEY LTD (IE); LYONS PATRIC) 27 June 2002 (2002-06-27) abstract page 1, paragraph 1 - page 10, paragraph 2	1-9

[ ] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 February 2004	26/02/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Teutloff, H

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/DE 03/03611

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 0217238	A	28-02-2002	AU	7631301 A	04-03-2002
			WO	0217238 A1	28-02-2002
			EP	1314140 A1	28-05-2003
WO 0005696	A	03-02-2000	AU	743933 B2	07-02-2002
			AU	3393399 A	10-02-2000
			BR	9912267 A	17-04-2001
			WO	0005696 A2	03-02-2000
			DE	59903476 D1	02-01-2003
			EP	1099204 A2	16-05-2001
			ES	2188244 T3	16-06-2003
			JP	2002521596 T	16-07-2002
WO 0249888	A	27-06-2002	AU	2244102 A	01-07-2002
			EP	1343664 A1	17-09-2003
			WO	0249888 A1	27-06-2002
			IE	20011092 A2	10-07-2002

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE 03/03611

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G07C9/00 B60R25/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G07C B60R

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	WO 02/17238 A (CROWHURST PETER ; PAVATICH FRANK (AU); BOSCH GMBH ROBERT (DE)) 28. Februar 2002 (2002-02-28) in der Anmeldung erwähnt das ganze Dokument	1-9
A	WO 00/05696 A (PAVATICH GIANFRANCO ; CROWHURST PETER (AU); BOSCH GMBH ROBERT (DE)) 3. Februar 2000 (2000-02-03) das ganze Dokument	1-9
A	WO 02/49888 A (GREENWOOD JEREMY JOHN ; LAND ROVER (GB); HI KEY LTD (IE); LYONS PATRIC) 27. Juni 2002 (2002-06-27) Zusammenfassung Seite 1, Absatz 1 - Seite 10, Absatz 2	1-9

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
19. Februar 2004	26/02/2004

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Teutloff, H

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/DE 03/03611

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
WO 0217238	A	28-02-2002	AU	7631301 A	04-03-2002
			WO	0217238 A1	28-02-2002
			EP	1314140 A1	28-05-2003
WO 0005696	A	03-02-2000	AU	743933 B2	07-02-2002
			AU	3393399 A	10-02-2000
			BR	9912267 A	17-04-2001
			WO	0005696 A2	03-02-2000
			DE	59903476 D1	02-01-2003
			EP	1099204 A2	16-05-2001
			ES	2188244 T3	16-06-2003
			JP	2002521596 T	16-07-2002
WO 0249888	A	27-06-2002	AU	2244102 A	01-07-2002
			EP	1343664 A1	17-09-2003
			WO	0249888 A1	27-06-2002
			IE	20011092 A2	10-07-2002